SISL-IT-POL-Patch Management and VAPT Policy

Version No: V 1.0

INTERNAL DOCUMENT

OCTOBER 2025

Document Control

Document Name	SISL-IT-POL-Patch Management and VAPT Policy
Abstract	This document describes Patch Management and VAPT Policy at Share India Group
Security Classification	Internal
Location	Share India Group– Delhi

Authorization		
Document Owner	Reviewed by	Authorized by
IT Team	Head – IT	Head – IT

Amendment Log				
Version	**Modification Date DD MMM YYYY**	**Section**	**A/M/D**	**Brief description of change**
1.0	30th October 2025	Initial Version	A	Final

Distribution list
Designated Officer (DO)
Information Security Steering Committee (ISSC)
ISMS Core Team
Auditors (Internal & External)
All users at Share India Group

Table of Content

1 Introduction

To properly secure SISL's information technology assets, the information security team shall assess the organization’s security stance periodically by conducting vulnerability assessments and penetration testing. The knowledge of these vulnerabilities shall help the organisation apply security fixes or other compensating controls to improve the security of the IT infrastructure.

Vulnerability analysis, also known as vulnerability assessment, is a process that defines, identifies, and classifies the security holes (vulnerabilities) in a computer, network, or communications infrastructure.

Penetration testing (also called pen testing) is the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit

2 Policy Statement

Conducting vulnerability assessment and penetration testing is a proactive step towards ensuring that any vulnerabilities existing in the IT infrastructure component is captured and addressed, thus reducing the risk of systems being compromised due to an attack.

3 Scope

The scope of the vulnerability assessment and penetration testing is:

1. Business Applications
2. Network devices
    a. Firewalls
    b. Routers
    c. Switches
    d. Wireless Access Devices
    e. Intrusion Prevention System
    f. Web Content Filtering
3. Servers
4. Critical laptops and desktops

4 Roles and Responsibilities

Sr. No.	Role	Responsibility
1.	Designated Officer (DO)	Owns the process
2.	IT HOD	Ensure that this policy is effectively implemented.
3.	IT Team (Infrastructure and Application)	Comply to this policy.

5 VAPT Policy

Vulnerability testing and penetration testing is required for systems hosting business critical information. Optionally, VAPT may be done for non-critical systems also.

5.1 Vulnerability Testing

- SISL shall conduct a vulnerability assessment of all their servers, network devices and applications on a quarterly basis.
- In case of a major change to the application, the underlying operating system or the backend database, a vulnerability scan shall be done prior to hosting the application in the production environment.
- In case a vulnerability scan fails, the scan shall be executed again till the time the testing is successfully done.
- The identified vulnerabilities shall be addressed as follows:
  - **Critical / High Risk vulnerabilities**: Rectification will be initiated within 1 month.
  - **Medium Risk vulnerabilities**: Rectification will be initiated within 2 months.
  - **Low Risk vulnerabilities**: will be resolved after addressing Critical and Medium Vulnerabilities.

5.2 Penetration Testing

- External penetration testing shall be performed at least once a year.
- External testing shall also be performed after any significant change in the IT infrastructure.
- Penetration testing shall minimally consist of network-layer and application-layer penetration tests.
- Exploitable vulnerabilities noted during penetration testing shall be corrected based on the criticality and an adequate retest shall be performed to demonstrate that identified exploit is addressed.

Capacity Planning exercise shall be carried out by the respective asset risk owner in consultation with the Information security management team taking into consideration the usage data. Penetration testing shall be conducted by CERT-In empanelled auditors or other competent third-party cybersecurity experts, in accordance with regulatory and internal compliance requirements.

6 Patch Management

Ensuring security of information and IT systems requires establishment and management of effective patch deployment system. This policy governs the management of patches required to control technical vulnerabilities of the Information and the IT systems being used in the SISL.

- Respective team(s) shall be responsible for ensuring deployment of patches in a controlled and timely manner. For this purpose, a governing procedure shall be established and shall be strictly adhered to.
- Team(s) shall also subscribe to relevant websites which provide information on latest vulnerabilities / security updates.
- All system, network and security devices shall be updated with latest security patches which are stable and tested.
- Each application server at the SISL shall be updated with the latest patches as recommended by OEM or respective software supplier as per change management procedure.
- All patches shall be appropriately tested before deployment, as applicable.
- Wherever technically feasible, patch management tools shall be used to assist in the uniform application of configurations, policies, and patches at an enterprise level.
- Patches shall be implemented as per their criticality.
- Patches shall be first implemented at test set-up to ensure minimal impact in case the implementation is unsuccessful.

The objective of this procedure is to define a set of processes for effective Patch Management across SISL IT Infrastructure.

#	Components	Team Responsible for updating patches	Recommending entity
1.	OS / Database for Trading Environment/Antivirus (EDR)	Sys Admin Team	Respective OEMs
2.	Firmware	Sys Admin / Network Team	Respective OEMs
3.	Router / Switches	Network Team	Respective OEMs

4.	Firewall / IDS / IPS	Network Team	Respective OEMs
5.	Local LAN Devices	Local IT Team	Respective OEMs

6.1 Patch Identification

- Team(s) check with respective recommending entity (OEM) as mentioned in the above table to avail the patches at least on quarterly basis.
- For Operating System / Database, the respective application vendor (OEM) provides the latest patches.
- For rest of the components, the teams download the patches from the respective OEM website.
- Confirmation about the patches been tested is received from the Infrastructure Team.
- Information on the patches which are not to be deployed shall be tested for impact and recommendation shall be obtained from the subject matter expert.
- In case of any problems in the functioning of the systems where the patches are installed, those patches are rolled back, and further implementation of that patch is stopped.
- Patches or upgrades are tested on separate machines or UAT environment.
- Observation period of the patch is of 15 days.
- A report is prepared for any UAT of patches and forwarded to the Head of Infrastructure Services.
- In case the patch installation is successful on UAT, the patches are individually deployed to all relevant systems after filling change management form.
- After the patch implementation is successful on all the relevant systems, a final report is prepared and forwarded to the Head of Infrastructure Services
- To be abreast on the latest vulnerabilities, IT security team will also subscribe on security advisory website (www.cert-in.org.in)

6.2 Analysis and Prioritization

- Post receipt of the patches, teams prepare patch management schedule for deployment of patches.
- The register will be accessible to the concerned team members for preparing the schedule.
- Schedule of deployment is prepared considering severity of patches.
- Information about criticality is obtained from OEM.
- Critical patches having active exploits are installed on a priority basis. Non-critical patches are installed during scheduled maintenance i.e. on a weekly basis.
- Teams get approval from Head of Infrastructure Services on the schedule prepared.

#	Components	Critical Patches	Non-Critical Patches
1.	OS / Database for Trading Environment/Antivirus (EDR)	-30 days	+90 days
2.	Firmware	-30 days	
3.	Router / Switches	-30 days	
4.	Firewall / IDS / IPS	-30 days	+90 days
5.	Local LAN devices	Immediately	+90 days

6.3 Testing and Approval

- UAT is performed as per the schedule.
- If UAT is unsuccessful, patching shall be delayed, and subject matter experts recommendation shall be sought for action and the schedule shall be updated for further implementation.
- Same procedure for approval and testing (as mentioned above) is followed till successful UAT.
- Post successful testing, the team informs all its stake holders on the same day with implementation plan to be deployed into production environment.
- CR (Change Request) is raised before implementing patches on production IT infrastructure (Primary Site and DR Site)
- As a part of CR initiation process, detailed Roll back plan is prepared to ensure quick and easy restoration of the system if patch has unintended/unexpected impact.
- Approval from the Head of Infrastructure Services is taken on change request.
- Team will inform the downtime to all users who may be impacted. (Non-Trading Hours)

6.4 Implementation

- Before deployment of patch in production, the team ensures proper backup of the servers / network devices.
- Patches are implemented as per the schedule as follows:
    - First at UAT
    - Then at DR site.
    - And then at Primary Site
- If installation is unsuccessful, roll back plan is referred to reverse changes.
- Root Cause Analysis (RCA) of failed patch is carried out by the respective team.
- RCA is submitted to the Head of Infrastructure Services for information purpose.

- Same procedure for approval and testing (as mentioned above) is followed till successful deployment.
- CR is closed by the respective team within next business working day from the date of successful deployment of patch.

6.5 Monitoring

On a daily basis, the team also verifies that all systems and applications are functioning normally, and that they comply with laid down security policies and guidelines.

7 Reference

Ref: - SISL-IT-PRO-Patch Management and VAPT Procedure

8 Policy Review Frequency

The policy shall be reviewed annually or when there is a major change within Share India Securities Limited environment.

9 Policy Exception

In case of any deviation against policy guidelines, Risk Acceptance form should be submitted to Designated Officer for approval.

10 Policy Violation Reporting Matrix

Any violation to the policy should be reported to Reporting Manager/Designated Officer

Level	Designation
Level 1	Employee's Reporting Manager
Level 2	Designated Officer
Level 3	MD & CEO